

17 MAG 3822

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Application for a  
Search Warrant for All Content and  
Other Information Associated with Ten  
Facebook Accounts at Premises  
Controlled by Facebook, Inc.

AGENT AFFIDAVIT

USAO Reference No. 2017R00116.

**Application for a Search Warrant  
for Stored Electronic Communications**

STATE OF NEW YORK     )  
                                      ) ss.  
COUNTY OF NEW YORK    )

JONATHAN PAGE, being duly sworn, deposes and states:

**I. Introduction**

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") for approximately two and a half years. For the last approximately two years, I have been assigned to the FBI's New York Joint Terrorism Task Force ("JTTF"). During this time period, I have participated in numerous investigations of unlawful activity, principally national security related matters and crimes relating to immigration fraud. During the course of these investigations, I have conducted or participated in surveillance, the introduction and debriefings of informants, and the execution of search warrants. Through my training, education, and experience, I have become familiar with various terrorist organizations, as well as the manner in which terrorists are recruited, receive training, and operate, and some of the methods that are used to conceal evidence of participation in such illegal activity. I have received training in the use of computer technology by terrorist networks and have participated in investigations involving the use of computers, the Internet, and social media by terrorists and terrorist organizations. Through my training and

experience, I have become familiar with some of the ways in which terrorist groups use the Internet, including social media and email, to promote their activities, recruit new members, and issue threats, and I have also participated in the execution of search warrants involving electronic evidence.

2. **Basis for Knowledge.** This Affidavit is based upon my participation in the investigation, my examination of reports and records, and my conversations with other law enforcement agents and other individuals, as well as my training and experience. Because this Affidavit is being submitted for the limited purpose of obtaining the Requested Information, it does not include all the facts that I have learned during the course of this investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated. In addition, unless otherwise indicated, statements by others referenced in this Affidavit were not necessarily made to me, but may have been provided to me by someone else to whom I have spoken or whose report I have read (and who in turn may have had either direct or indirect knowledge of the statement). Similarly, unless otherwise indicated, information in this Affidavit resulting from surveillance does not necessarily set forth my personal observations, but may have been provided to me by other law enforcement agents who observed the events, and to whom I have spoken or whose report I have read.

## **II. The Provider, the Target Accounts, and the Subject Offenses**

3. I am submitting this Affidavit in support of an application for a search warrant directed to Facebook, Inc. ("Facebook" or the "Provider"), with offices in Menlo Park, California, relating to the following **Target Accounts**, each of which is maintained at premises controlled by the Provider:

- a. The Facebook account with identification number 100013341277222, subscriber name "Ali Kourani," and subscriber email "jacob.kouran@gmail.com" ("**Target Account-1**");
- b. The Facebook account with identification number 503619729, subscriber name "Ali Koran," and subscriber emails "ali.m.kourani@gmail.com" and "aliku@hotmai.com" ("**Target Account-2**");
- c. The Facebook account with identification number 100007817464240, username "Ali Kourani," and other subscriber information unknown ("**Target Account-3**");
- d. The Facebook account with identification number 1602196647, username "Bilal Kourani," and other subscriber information unknown ("**Target Account-4**");
- e. The Facebook account with identification number 547052076, username "Hussein Fares," and other subscriber information unknown ("**Target Account-5**");
- f. The Facebook account with identification number 1656786545, username "Youssef A Fares," and other subscriber information unknown ("**Target Account-6**");
- g. The Facebook account with identification number 54700693, username "Ali Fares," and other subscriber information unknown ("**Target Account-7**");
- h. The Facebook account with identification number 1417299773, username "علي شاهين" and other subscriber information unknown ("**Target Account-8**");
- i. The Facebook account with identification number 564327740, username "Ali Kourani," and other subscriber information unknown ("**Target Account-9**"); and
- j. The Facebook account with identification number 551231921, username "Mohammad Sadek," and other subscriber information unknown ("**Target Account-10**").

4. Based on my training, experience, and participation in this investigation, I know the following about Facebook:

a. Facebook owns and operates a free-access, social-networking website of the same name that can be accessed at <http://www.facebook.com>. Facebook allows Internet users to establish accounts with Facebook, which they can use to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

b. Facebook asks users to provide basic contact information to Facebook, either during the registration process or thereafter. This information may include the user's full name, birth date, contact e-mail addresses, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers. Facebook also assigns a user identification number to each account.

c. Facebook users can select different levels of privacy for the communications and information associated with their Facebook accounts. By adjusting these privacy settings, a Facebook user can make information available only to himself or herself, to particular Facebook users, to all Facebook users, or to anyone with access to the Internet, including people who are not Facebook users. Facebook accounts also include other account settings that users can adjust, to control, for example, the types of notifications they receive from Facebook.

d. Facebook users may join one or more groups or networks to connect and interact with other users who are members of the same group or network. A Facebook user can also connect directly with individual Facebook users by sending each user a "Friend Request." If the recipient of a "Friend Request" accepts the request, then the two users will become "Friends" for purposes of Facebook and can exchange communications or view information about each other. Each Facebook user's account includes a list of that user's "Friends" and a "Mini-Feed," which

highlights information about the user's "Friends," such as profile changes, upcoming events, and birthdays.

e. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

f. Facebook has a Photos application, where users can upload an unlimited number of albums and photos. Another feature of the Photos application is the ability to "tag" (i.e., label) other Facebook users in a photo or video. When a user is tagged in a photo or video, he or she receives a notification of the tag and a link to see the photo or video. For Facebook's purposes, a user's "Photoprint" includes all photos uploaded by that user that have not been deleted, as well as all photos uploaded by anyone else that have that user tagged in them.

g. Facebook users can exchange private messages on Facebook with other users. These messages, which are similar to e-mail messages, are sent to the recipient's "Inbox" on Facebook, which also stores copies of messages sent by the recipient, as well as other information. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile.

h. Facebook Notes is a blogging feature available to Facebook users, and it enables users to write and post notes or personal web logs (“blogs”), or to import their blogs from other services, such as Xanga, LiveJournal, and Blogger.

i. The Facebook Gifts feature allows users to send virtual “gifts” to their friends that appear as icons on the recipient’s profile page. Gifts cost money to purchase, and a personalized message can be attached to each gift. Facebook users can also send each other “pokes,” which are free and simply result in a notification to the recipient that he or she has been “poked” by the sender.

j. Facebook also has a Marketplace feature, which allows users to post free classified ads. Users can post items for sale, housing, jobs, and other items on the Marketplace.

k. In addition to the applications described above, Facebook also provides its users with access to thousands of other applications on the Facebook platform. When a Facebook user accesses or uses one of these applications, an update about that user’s access or use of that application may appear on the user’s profile page.

l. Facebook uses the term “Neoprint” to describe an expanded view of a given user profile. The “Neoprint” for a given user can include the following information from the user’s profile: profile contact information; Mini-Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends’ Facebook user identification numbers; groups and networks of which the user is a member, including the groups’ Facebook group identification numbers; future and past event postings; rejected “Friend” requests; comments; gifts; pokes; tags; and information about the user’s access and use of Facebook applications.

m. Facebook also includes a search function that enables its users to search for other Facebook users, conduct web searches through Facebook, among other searches. Facebook stores searches performed by users through their Facebook accounts.

n. Facebook also retains Internet Protocol (“IP”) logs for a given user ID or IP address. These logs may contain information about the actions taken by the user ID or IP address on Facebook, including information about the type of action, the date and time of the action, and the user ID and IP address associated with the action. For example, if a user views a Facebook profile, that user’s IP log would reflect the fact that the user viewed the profile, and would show when and from what IP address the user did so.

o. Social-networking providers like Facebook typically retain additional information about their users’ accounts, such as information about the length of service (including start date), the types of service utilized, and the means and source of any payments associated with the service (including any credit card or bank account number). In some cases, Facebook users may communicate directly with Facebook about issues relating to their account, such as technical problems, billing inquiries, or complaints from other users. Social networking providers like Facebook typically retain records about such communications, including records of contacts between the user and Yahoo’s support services, as well as records of any actions taken by the provider or user as a result of the communications.

p. Facebook typically maintains preserved copies of the foregoing categories of records with respect to an account, for at least 90 days, upon receiving a preservation request from the Government pursuant to 18 U.S.C. § 2703(f).

5. As detailed below, there is probable cause to believe that the Target Accounts contain evidence, fruits, and instrumentalities of violations of: (i) Title 18, United States Code, Section

2339B (providing material support or resources to designated foreign terrorist organizations); (ii) Title 18, United States Code, Section 2339D (receipt of military-type training from designated foreign terrorist organizations); (iii) Title 18, United States Code, Section 924(c) (firearms offenses related to crimes of violence); (iv) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (v) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the "Subject Offenses"). This affidavit is based upon my personal knowledge, my review of documents and other evidence, and my conversations with other law enforcement officers, as well as my training and experience concerning the use of email in criminal activity. Because this affidavit is being submitted for the limited purpose of establishing probable cause, it does not include all the facts I have learned during my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

### **III. Jurisdiction to Issue the Requested Warrant**

6. Pursuant to Title 18, United States Code, Sections 2703(a), (b)(1)(A) & (c)(1)(A), the Government may require a provider of an electronic communications service or a remote computing service, such as the Provider, to disclose all stored content and all non-content records or other information pertaining to a subscriber, by obtaining a warrant issued using the procedures described in the Federal Rules of Criminal Procedure.

7. A search warrant under Section 2703 may be issued by "any district court of the United States (including a magistrate judge of such a court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

8. When the Government obtains records under Section 2703 pursuant to a search warrant, the Government is not required to notify the subscriber of the existence of the warrant. 18 U.S.C. § 2703(a), (b)(1)(A), (c)(2) & (3). Additionally, the Government may obtain an order precluding the Provider from notifying the subscriber or any other person of the warrant, for such period as the Court deems appropriate, where there is reason to believe that such notification will seriously jeopardize an investigation. 18 U.S.C. § 2705(b).

#### **IV. Facts Establishing Probable Cause**

##### **A. Hizballah and the Islamic Jihad Organization (IJO)**

9. Based on my training, experience, and participation in this and related investigations, I am aware of the following:

a. Hizballah (or Hezbollah)—which is Arabic for “Party of God”—is based in Lebanon. Hizballah was founded in the early 1980s with support from Iran, after the 1982 Israeli invasion of Lebanon. Hizballah’s mission includes establishing a fundamentalist Islamic state in Lebanon.

b. The Islamic Jihad Organization (“IJO”), which is also known as the External Security Organization (“ESO”) and “910,” is a component of Hizballah responsible for the planning and coordination of attacks by Hizballah outside Lebanon.

c. Since its formation, Hizballah has been responsible for numerous terrorist attacks that have killed hundreds, including the 1983 bombing of the United States Marine barracks in Lebanon, which killed 241 Marines; the 1983 bombing of the United States Embassy in Beirut, which killed 24 people; the 1985 hijacking of TWA flight 847, which killed at least one U.S. citizen; the 1992 bombing of the Israeli Embassy in Argentina, which killed 29 people; and the 1994 bombing of a Jewish cultural center in Buenos Aires, which killed 95 people.

d. In 1995, the United States Department of State designated Hizballah as a Foreign Terrorist Organization, pursuant to section 219 of the Immigration and Nationality Act, and it remains so designated today.

e. In 2001, pursuant to Executive Order 13,224, the United States named Hizballah as a Specially Designated Global Terrorist entity.

f. In July and August 2006, Hizballah and Israel engaged in armed conflict, resulting in numerous casualties, after an incident on or about July 12, 2006 when Hizballah attacked Israeli Defense Force personnel. A ceasefire brokered by the United Nations went into effect on August 14, 2006.

g. In January 2012, a Hizballah operative named Hussein Atris was detained in Thailand as he tried to board a flight at Bangkok Airport. Atris subsequently led law enforcement personnel to a cache of nearly 10,000 pounds of urea-based fertilizer and 10 gallons of ammonium nitrate (stored in First Aid ice packs)—chemicals that I know, based on my training and experience, can be used to construct explosives—stored in a commercial building near Bangkok.

h. In July 2012, a suicide bomber detonated explosives on a bus transporting Israeli tourists in the vicinity of an airport in Burgas, Bulgaria. Six people were killed and 32 others were injured. Bulgarian authorities subsequently made public statements relating to evidence linking the attack to Hizballah.

i. In May 2015, a Hizballah operative named Hussein Bassam Abdallah was arrested in Cyprus after Cypriot authorities seized from an apartment rented by Abdallah approximately 8.2 tons of ammonium nitrate, at least some of which was stored in First Aid ice packs manufactured by the same company, and with the same lot number, as the First Aid ice packs with ammonium nitrate that were seized in Thailand in January 2012. *See*, paragraph 9(g),

*supra*. Abdallah was subsequently convicted in Cyprus of charges relating to surveillance of Israeli tourist targets.

**B. Ali Kourani**

10. Based on my review of documents and information maintained by federal and state authorities in the United States, I am aware of the following:

- a. Ali Kourani (“Kourani”) was born in Bint Jubayl, Lebanon in 1984.
- b. In 2003, Kourani lawfully entered the United States from Cyprus.
- c. In approximately August 2008, Kourani submitted an application for naturalization in the United States (the “Naturalization Application”). In the Naturalization Application, Kourani declared, among other things, that:
  - i. He had never “been a member of or in any way associated (*either directly or indirectly*) with . . . [a] terrorist organization.”
  - ii. He had never “given false or misleading information to any U.S. government official while applying for any immigration benefit . . . .”
  - iii. He had never “lied to any U.S. government official to gain entry or admission into the United States.”
- d. On or about April 15, 2009, the Naturalization Application was approved, and Kourani became a naturalized citizen of the United States.
- e. In or about April 2009, Kourani obtained a United States passport.
- f. Based on passports used by Kourani and information from law enforcement databases, Kourani’s foreign travel has included the following:
  - i. On or about July 4, 2010, Kourani entered Lebanon. On or about August 17, 2010, Kourani returned to the United States.

- ii. On or about June 23, 2011, Kourani entered Geneva, Switzerland; and on or about October 17, 2011, Kourani departed Lebanon (the “2011 Lebanon Trip”).
- iii. On or about June 12, 2012, Kourani entered Lebanon.
- iv. On or about July 13, 2012, Kourani entered Lebanon.
- v. On or about December 26, 2012, Kourani entered Lebanon; and on or about January 12, 2013, Kourani exited Lebanon (the “2012 Lebanon Trip”).
- vi. On or about May 17, 2014, Kourani entered Canada; and on or about July 10, 2014, Kourani returned to the United States (the “2014 Canada Trip”).
- g. In or about April 2013, Kourani obtained a United States passport card.
- h. On or about September 18, 2015, when Kourani attempted to enter the United States at John F. Kennedy International Airport, law enforcement personnel identified a micro SD card secreted under a travel sticker affixed to Kourani’s U.S. passport.<sup>1</sup>

**C. Kourani’s 2016 Interviews with the FBI**

11. Based on my participation in this investigation, I know that in or about 2016, Kourani was approached by United States authorities on several occasions. Based on my review of reports relating to those interviews, Kourani made the following statements, in substance and in part:

- a. Kourani repeatedly denied membership in, or affiliation with, Hizballah.
- b. Kourani’s family name was akin to the “Bin Ladens of Lebanon.”
- c. Another one of Kourani’s brothers, Qasem, had resided in the United States but later became a political leader and “face of Hizballah” in Yatar, Lebanon.
- d. Husam Kourani, described by Kourani at various times during the interviews as a friend or cousin, was a member and “soldier” of Hizballah who moved to the United States,

---

<sup>1</sup> Due to technological problems, law enforcement did not obtain the contents of the SD card.

and then moved to Sao Paolo, Brazil in approximately 2005 after being approached by authorities in the United States.<sup>2</sup>

e. Muhammad Kourani (no relation) was the son of a former senior member of Hizballah known as Sheikh Hussein Kourani, and the husband of Kourani's sister, Layla Kourani.

f. Kourani was in Yater, Lebanon in 2006 when war broke out with Israel. *See* paragraph 9(f), *supra*. Kourani and certain of his relatives fled to Damascus, Syria, and then returned to New York. A home belonging to Kourani's father was destroyed in the conflict.

#### **D. Kourani's 2017 Admissions to the FBI**

12. In approximately March 2017, after an attorney (the "Attorney") contacted the FBI on behalf of Kourani and requested a meeting, Kourani participated in a series of interviews with FBI personnel. The Attorney was present during the interviews, and Kourani explained, in substance and in part, that he wished to provide information to the FBI in the hope of obtaining financial support as well as immigration benefits for certain of his relatives in Lebanon and Canada. No promises were made to Kourani regarding the availability of such benefits.

13. Based on my review of reports relating to interviews of Kourani beginning in approximately March 2017, as well as conversations with another FBI agent who participated in the interviews, I know that Kourani made the following statements, in substance and in part:

a. In approximately 2000, Kourani attended a 45-day Hizballah "boot camp" in Lebanon. Kourani was approximately 16 at the time, and he was permitted to attend because of his family's connections to a high-ranking Hizballah official named Haider Kourani. During the

---

<sup>2</sup> Records maintained by the Department of Homeland Security suggest that Husam Kourani took a commercial flight from the United States to Bogota, under an assumed name, on June 29, 2007.

training, Kourani was taught to fire AK-47s and rocket launchers, as well as basic military tactics, by Hizballah personnel wearing uniforms.

b. Between approximately 2008 and approximately September 2015,<sup>3</sup> Kourani was a member of the IJO, which is responsible for “black ops” on behalf of Hizballah and “the Iranians.” By the time Kourani was a member of the IJO, and thereafter, he understood that Hassan Nasrallah, the Secretary General of Hizballah, operated IJO and reported directly to Ali Khamenei, the Supreme Leader of Iran.

c. Sheikh Hussein Kourani recruited Kourani to join the IJO in Lebanon in approximately 2010. *See* paragraph 10(f)(i) *supra* (describing Kourani’s 2010 travel to Lebanon). During subsequent meetings in Lebanon with members or associates of Hizballah, Kourani was asked questions about his background and provided with training regarding, among other things, resisting interrogation. Kourani was also trained to gather and report on details about airport security, such as information relating to airport security personnel and the location of security cameras.

d. Following Kourani’s initial IJO training sessions, Kourani was taken to a meeting in Lebanon with a man named “Fadi” or “Hajj” (“Fadi”), who acted as Kourani’s handler while Kourani was a member of the IJO. Fadi told Kourani that he was expected to be operational within the United States, but could also be sent to another location or recalled to Lebanon if a war broke out.

---

<sup>3</sup> In earlier interviews in 2017, Kourani stated, in substance and in part, that he was recruited to join IJO in approximately 2010. He subsequently corrected the date, to 2008, and explained that he had lied initially because he believed that the truthful information about his recruitment and membership in the organization could jeopardize his status as a naturalized citizen.

e. One of Fadi's initial taskings to Kourani was to identify and assess military and intelligence targets in the New York City area, as well as a source of firearms for Hizballah to cache weapons in the City. In response to that tasking, Kourani conducted surveillance, some of which he videotaped, of an armory facility on 27th Street in Manhattan between Fifth Avenue and Park Avenue. Kourani also identified an FBI office in Manhattan and a Secret Service office in Brooklyn.<sup>4</sup>

f. In approximately 2011, Kourani returned to Lebanon after his initial mission. *See* paragraph 10(f)(ii), *supra* (describing an October 2011 exit from Lebanon). Kourani transported some of the products of his surveillance back to Lebanon on a micro SD card. *See* paragraph 10(h), *supra* (describing micro SD card secreted in Kourani's passport upon returning to the United States in September 2015).

g. In Lebanon, Kourani identified to a Hizballah handler other than Fadi the FBI office in Manhattan and the Secret Service office in Brooklyn. Kourani provided images from Google Earth of those buildings, as well as video of the armory facility in Manhattan. Kourani provided Fadi with approximately 10 telephone numbers of individuals Kourani believed could supply firearms, but Fadi indicated that the contacts were not sufficiently reliable. Kourani also provided Fadi with information regarding John F. Kennedy International Airport, including the manner in which passengers disembark from planes, are screened at customs, and collect luggage, as well as the locations of security personnel, security cameras, and magnetometers.

---

<sup>4</sup> During one of the interviews, Kourani confirmed by reviewing photographs that he had provided Fadi with surveillance information relating to 26 Federal Plaza (which includes FBI offices), the Army National Guard Building at 2366 5th Avenue in Manhattan, the U.S. Army 69th Regiment Armory at 68 Lexington Avenue in Manhattan, and the U.S. Secret Service Office Building at 335 Adams Street in Brooklyn.

h. In approximately July 2011, Kourani attended a Hizballah military training camp, located at Birkat Jabrur, Lebanon, where he was trained to use—and fired—several weapons (including AK-47s, MP-5 sub-machineguns, and grenade launchers).

i. During the 2011 Lebanon Trip, Kourani was tasked with purchasing equipment, such as drones, night-vision goggles, and high-powered cameras, so that Hizballah could work with Iranian or Russian associates to duplicate the technology. Kourani told the FBI, however, that he did not purchase any of these items.

j. Also during the 2011 Lebanon Trip, Sheikh Hussein Kourani told Kourani that he had just met with Mohammad Hamadi, a man Kourani described as a prominent member of Hizballah who had participated in the plot to hijack TWA flight 847, *see* paragraph 9(h), *supra*. Sheikh Hussein Kourani told Kourani that Hamadi still worked for Hizballah after serving a significant term of imprisonment in Germany, and should inspire Kourani to “man up.”

k. In approximately December 2012, while Kourani was in Lebanon, he spoke with Fadi about the July 2012 bombing in Bulgaria. *See* paragraph 10(f)(iii)-(v), *supra*. Fadi was critical of some aspects of the operation, and Kourani believed based on Fadi’s comments that he was involved in coordinating the attack.

l. In approximately 2012 or 2013, Fadi directed Kourani to obtain a U.S. passport card so that, in the event his U.S. passport was seized, he could use the passport card to transit the U.S. border. *See* paragraph 10(f)(iii)-(v), *supra* (describing multiple entries into Lebanon in 2012). Kourani confirmed that his April 2013 application for a U.S. passport card, *see* paragraph 10(g), *supra*, was submitted in response to this tasking from Fadi.

m. Kourani was trained to use digital storage media, such as USB drives, to transport pictures and data back to Lebanon. He was also trained to use email accounts to

communicate regarding operational activities and to send information back to Lebanon. Kourani said that he used the email addresses, including ali.m.kourani@gmail.com and alikuku@hotmail.com, to communicate with Fadi using predetermined codes that they discussed in person. Kourani stated that he would regularly delete communications with Hizballah operatives, including his handlers, immediately upon reading them.

n. Fadi tasked Kourani with seeking information regarding the Israeli Consulate in New York City and Jewish businessmen in the area who were current or former members of the Israeli Defense Forces (“IDF”), especially those who were veterans of the 2006 War. Kourani understood that such individuals could be targeted by the IJO for either recruitment or assassination, and he said that he located people in New York associated with the IDF by searching the LinkedIn website using his account.

o. Kourani further provided information regarding individuals of interest, some of whom he identified as possible ESO operatives, and others whom he identified as Hizballah sympathizers with possible ties to Hizballah militia or clerical members. Specific information provided by Kourani regarding certain of these individuals is detailed further in Section E, *infra*. Kourani additionally indicated that several of these individuals are located in the United States, Canada, and Lebanon.<sup>5</sup>

14. On or about May 17, 2017, the Attorney, referenced in paragraph 12, *supra*, informed the FBI, in substance and in part, that Kourani intends to soon leave the United States, and return to Lebanon to reside there.

---

<sup>5</sup> Kourani separately stated that he believed ESO would smuggle explosives into the United States from Canada.

**E. The Target Accounts**

15. Based on my training, experience, and participation in this and related investigations, I am aware of the following tradecraft and communications security practices of Hizballah and IJO:

a. Hizballah and IJO personnel often use Facebook—including the private communications feature associated with Facebook accounts—to communicate for operational purposes;

b. Hizballah and IJO personnel sometimes establish multiple Facebook accounts, some of which can be accessed by their handlers as well, to communicate regarding their operations, activities, and status;

c. Consistent with Kourani's statements to the FBI regarding deleting operational communications, *see* paragraph 13(m), *supra*, Hizballah and IJO personnel sometimes delete electronic communications to destroy evidence of their activities;

d. When Hizballah and IJO personnel become concerned that a method of communication has been compromised by a law enforcement or counterintelligence adversary, Hizballah and IJO personnel typically deactivate and/or purge the contents of the account, *see* paragraph 16(b), *infra* (discussing deactivation of **Target Account-2**); Facebook, however, sometimes maintains such contents and related metadata notwithstanding user efforts to destroy it.

16. Based on my review of information relating to **Target Account-1** and **Target Account-2**, which was provided by Facebook in response to an order issued pursuant to Title 18, United States Code, Section 2703(d), I know, among other things, the following:

a. **Target Account-1** appears to have been used by Kourani. The account is subscribed in Kourani's name, was registered in or about August 2016, and remains active. **Target Account-1** also contains uploaded photos and videos.

b. Kourani identified **Target Account-2** to the FBI in 2017 as a Facebook account that he utilized. The subscriber information for **Target Account-2** lists the name “Ali Koran” as well as the two email addresses that Kourani told the FBI he used for IJO-related activities: ali.m.kourani@gmail.com and alikuku@hotmail.com. The account was registered in or about April 2007 and deactivated in or about March 2016. **Target Account-2** further contains photos uploaded during the approximate time period of the 2012 Lebanon Trip, *see* paragraph 10(f)(v), *supra*, and the 2014 Canada Trip, *see* paragraph 10(f)(vi), *supra*.

c. **Target Account-3** appears to be associated with Kourani, as it contains the username “Ali Kourani.” On or about March 3, 2014, **Target Account-2** sent **Target Account-3** a message, which in my training and experience is consistent with Hizballah and IJO operational tradecraft and may reflect, among other things, a communication between Kourani and one of his IJO handlers.

d. **Target Account-4**, with username “Bilal Kourani,” appears to be affiliated with an individual who Kourani identified to the FBI as Bilal Kourani.

i. Specifically, on or about April 26, 2017, Kourani stated to the FBI, in substance and in part, that Bilal Kourani attended a Hizballah training camp, and recently immigrated to the United States. Kourani further stated during the interview that Bilal Kourani’s brother, Hassan Kourani, maintains close relationships to prominent Shia clerics in Lebanon who are affiliated with Hizballah.

ii. On or about October 23, 2011, **Target Account-2** (Ali Koran) and **Target Account-4** exchanged approximately 18 messages, all of which have been deleted from **Target Account-2** in a manner consistent with Hizballah and IJO tradecraft, *see* paragraph 15(c)-

(d), *supra*. Of note, these messages were exchanged 6 days after Kourani returned from the 2011 Lebanon Trip, *see* paragraph 10(f)(ii), *supra*.

iii. On or about May 28, 2013, **Target Account-4** sent a message to **Target Account-2**. Kourani was traveling outside of the United States during this time, *see* paragraph 10(f)(iv), *supra*.

e. **Target Account-5**, with username “Hussein Fares,” appears to be affiliated with an individual who Kourani identified to the FBI as Hussein Lufti Fares. On or about April 26, 2017, Kourani identified Hussein Fares to the FBI as an affiliate of Hizballah. In or around the period of August 13, 2014 through August 24, 2014, **Target Account-2** (Ali Koran) and **Target Account-5** exchanged four messages.

f. **Target Account-6**, with username “Youssef A Fares,” appears to be affiliated with an individual who Kourani identified as Youssef Ali Fares. On or about April 26, 2017, Kourani identified Youssef Ali Fares to the FBI as a potential member of IJO, who is living in the New York area. Kourani stated, in substance and in part, that Fares has many connections to prominent Shia clerics in Lebanon who are Hizballah affiliates. On or about March 12, 2017, **Target Account-1** (Ali Kourani) sent **Target Account-6** a message.

g. **Target Account-7** has username “Ali Fares,” which is a variant on the name “Youssef Ali Fares,” the man Kourani identified to the FBI as a potential member of IJO. *See* paragraph 16(f), *supra*. On or about December 14, 2016, **Target Account-1** (Ali Kourani) sent **Target Account-7** a message.

h. **Target Account-8**, has username “شاهين علي,” which is “Ali Shahin” in transliterated Arabic. On or about April 26, 2017, Kourani stated to the FBI, in substance and in part, that the Shahin family is closely, and covertly, affiliated with Hizballah. Kourani indicated

that at least one member of the Shahin family, “Mousa Shahin” lives in Brooklyn, New York, and is involved in fraudulent businesses. Kourani stated that Ali Shahin works in the New York City area. On or about February 16, 2017, **Target Account-1** (Ali Kourani) sent **Target Account-8** a message.

i. **Target Account-9** appears to have been used by Kourani, as it contains the username “Ali Kourani,” which in my training and experience is consistent with Hizballah and IJO operational tradecraft and may reflect, among other things, a communication between Kourani and one of his IJO handlers. **Target Account-9** communicated with **Target Account-1** (Ali Kourani) and **Target Account-2** (Ali Koran) on or about the following dates, and many of the communications were deleted from **Target Account-2** in a manner consistent with IJO tradecraft, *see* paragraph 15(c)-(d), *supra*.

i. On or about June 5, 2011, **Target Account-9** sent **Target Account-2** three messages, all of which were deleted from **Target Account-2**. Of note, these messages occurred approximately 18 days before the 2011 Lebanon Trip.

ii. During the 2011 Lebanon Trip, **Target Account-9** and **Target Account-2** exchanged four messages, all of which were deleted from **Target Account-2**.

iii. In the approximately 30 days following Kourani’s return to the United States from the 2011 Lebanon Trip, **Target Account-9** and **Target Account-2** exchanged approximately 25 messages, all of which were deleted from **Target Account-2**.

iv. On or about January 8, 2012, **Target Account-9** and **Target Account-2** exchanged approximately five messages, all of which were deleted from **Target Account-2**.

v. On or about March 31, 2012, **Target Account-9** sent a message to **Target Account-2**, which was deleted from **Target Account-2**.

vi. On or about November 6, 2013, **Target Account-9** and **Target Account-2** exchanged approximately three messages, all of which were deleted from **Target Account-2**.

vii. On or about February 21, 2017, **Target Account-1** sent a message to **Target Account-9**.

j. **Target Account-10** contains the username "Mohammad Sadek." Approximately seven days before the 2011 Lebanon Trip, **Target Account-2** (Ali Koran) exchanged approximately 54 messages with **Target Account-10**. Additionally, during the course of the 2011 Lebanon Trip, **Target Account-2** exchanged approximately 44 messages with **Target Account-10**. All of the messages references in this subparagraph were deleted from **Target Account-2** in a manner consistent with Hizballah and IJO tradecraft, *see* paragraph 15(c)-(d), *supra*.

17. In sum, based on the foregoing analysis, I respectfully submit that:

a. **Target Account-1** through **Target Account-9** appear to be associated with Kourani, or with individuals whom Kourani identified as being members or associates of Hizballah;

b. **Target Account-10** was in contact with **Target Account-2** relatively frequently, in proximity to the 2011 Lebanon Trip during which Kourani received military-type training, and may therefore provide evidence of, *inter alia*, Kourani's geolocation and activities in that timeframe;

c. Although nearly 100 messages exchanged between **Target Account-2** and **Target Account-10** around the time of Kourani's operational travel were deleted from **Target Account-2**, it may be possible to obtain the content of those messages or associated metadata from **Target Account-10**.

d. The manner in which the **Target Accounts** were used, as described above, is consistent with Hizballah or IJO tradecraft, such as trying to purge accounts (**Target Account-2**), or delete particular message related to operational or other criminal activities;

e. Even if Facebook does not maintain the content of messages that its users deleted from the **Target Accounts**, evidence of tradecraft reflected by the fact of the deletions may serve as evidence relating to the Subject Offenses, and Facebook may also have IP and geolocation information relating to the messages or associated logins to the **Target Accounts**.

#### **V. Evidence, Fruits and Instrumentalities in Target Accounts**

18. Based on my training and experience, I am familiar with the means through which persons communicate with each other in the course of committing and seeking to conceal terrorism offenses, including their receipt of training to engage in acts of terrorism. These methods often include communications by email and through the Internet using social networking sites, such as Facebook. Moreover, based on my training and experience, I know that social media can be used to identify evidence regarding training received by suspects, methods of entry into a country, travel plans, and the source and method for obtaining training. Based on my training and experience, I know that social media can also be used to identify other individuals who similarly aspire to engage in acts of terrorism. Furthermore, based on my training and experience in other terrorism investigations, I know that individuals aspiring to conduct acts of terrorism often travel to regions of the globe such as Lebanon to receive training from military-type training from terrorists and terrorist organizations, including in how to construct and detonate explosives.

19. Based upon the foregoing, I respectfully submit there is probable cause to believe that information stored on the Provider's servers associated with the **Target Accounts** will contain evidence, fruits, and instrumentalities of the Subject Offenses, as more fully described in Section

II of Attachment A to the requested warrant, a copy of which shall not be transmitted to the Provider. In particular, I believe the **Target Accounts** are likely to contain, among other things, the following information:

- a. Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;
- b. evidence of the identity(ies) of the user(s) of the Target Accounts;
- c. evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- d. evidence of participation in the Subject Offenses by the user(s) of the Target Accounts and others, including records and photographs relating to travel and financial transactions in furtherance of the Subject Offenses;
- e. evidence related to banks and other financial institutions at which the user(s) of the Target Accounts conducts business, including, potentially, transactions in furtherance of the Subject Offenses;
- f. evidence of other online accounts and email addresses used by the user(s) of the Target Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- g. passwords or other information needed to access user's computer or other online accounts.

20. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for service of a search warrant issued under § 2703, or for the collection or production of responsive records. Accordingly, the warrant requested herein will be transmitted to the Provider, which will be directed to produce a digital copy of any responsive records to law enforcement personnel within 24 hours of the date of service. Law enforcement personnel (including, in addition to law enforcement officers and agents, and depending on the nature of the ESI and the status of the investigation and related proceedings, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) will retain the records and review them for evidence, fruits, and instrumentalities of the Subject Offenses as specified in Section III of Attachment A to the requested warrant.

21. In conducting this review, law enforcement personnel may use various methods to locate evidence, fruits, and instrumentalities of the Subject Offenses, including but not limited to undertaking a cursory inspection of all content associated with the **Target Accounts**. This method is analogous to cursorily inspecting all the files in a file cabinet in an office to determine which paper evidence is subject to seizure. Although law enforcement personnel may use other methods as well, to the extent applicable, including keyword searches, I know that keyword searches and similar methods are typically inadequate to detect all information subject to seizure. As an initial matter, keyword searches work only for text data, yet many types of files commonly associated with emails, including attachments such as scanned documents, pictures, and videos, do not store data as searchable text. Moreover, even as to text data, keyword searches cannot be relied upon to capture all relevant communications in an account, as it is impossible to know in advance all of the unique words or phrases that investigative subjects will use in their communications, and

consequently there are often many communications in an account that are relevant to an investigation but that do not contain any keywords that an agent is likely to search for.


**VI. Request for Non-Disclosure, Sealing Order, and Order for Expedited Compliance**

22. The full existence and scope of this ongoing criminal investigation are not publicly known. As a result, premature public disclosure of this affidavit or the requested warrant could alert potential criminal targets that they are under investigation, causing them to destroy evidence, flee from prosecution, or otherwise seriously jeopardize the investigation. In particular, the targets could easily delete, encrypt, or otherwise conceal digital evidence from law enforcement were they to learn of the Government's investigation.

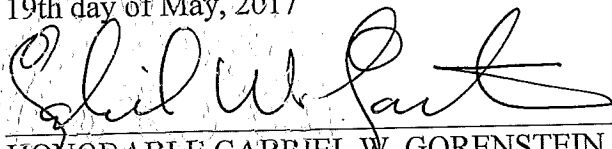
23. Accordingly, there is reason to believe that, were the Provider to notify the subscriber(s) or others of the existence of the requested warrant, the investigation would be seriously jeopardized. Pursuant to 18 U.S.C. § 2705(b), I therefore respectfully request that the Court direct the Provider not to notify any person of the existence of the warrant for a period of 180 days from issuance, subject to extension upon application to the Court, if necessary.

24. For similar reasons, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise, except that the Government be permitted without further order of this Court to provide copies of the warrant and affidavit as need be to personnel assisting it in the investigation and prosecution of this matter, and to disclose those materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

25. Based on the foregoing, and in particular, the Attorney's statements that Kourani intends to flee to Lebanon imminently, I respectfully request that the Court require the Service Provider to provide the Requested Information within twenty-four hours of service of the Order.

  
Special Agent Jonathan Page  
Federal Bureau of Investigation

Sworn to before me this  
19th day of May, 2017

  
HONORABLE GABRIEL W. GORENSTEIN  
United States Magistrate Judge  
Southern District of New York

17 MAG 3822

UNITED STATES DISTRICT COURT  
SOUTHERN DISTRICT OF NEW YORK

In the Matter of an Application for a  
Search Warrant for All Content and  
Other Information Associated with  
Ten Facebook Accounts at Premises  
Controlled by Facebook, Inc.

**SEARCH WARRANT**

TO: Facebook, Inc. ("Provider")

Federal Bureau of Investigation ("Investigative Agency")

**1. Warrant.** Upon an Affidavit of a federal law enforcement officer in connection with an investigation being conducted by the Investigative Agency, and pursuant to the provisions of the Stored Communications Act, 18 U.S.C. § 2703(b)(1)(A) and § 2703(c)(1)(A), and the relevant provisions of Federal Rule of Criminal Procedure 41, the Court hereby finds that there is probable cause to believe that the 10 Facebook accounts described in Attachment A hereto, which are controlled and maintained at premises controlled by the Provider, a company headquartered in Menlo Park, California, contains evidence, fruits, and instrumentalities of crime, all as specified in Attachment A hereto. Accordingly, the Provider is hereby directed to provide to the Investigative Agency, within 24 hours of the date of service of this Warrant and Order, <sup>if feasible,</sup> the records specified in Section II of Attachment A hereto, for subsequent review by law enforcement personnel as authorized in Section III of Attachment A, a copy of which shall not be transmitted to the Provider. The Government is required to serve a copy of this Warrant and Order forthwith. The Warrant and Order may be served via electronic transmission or any other means through which the Provider is capable of accepting service.

**2. Non-Disclosure Order.** Pursuant to 18 U.S.C. § 2705(b), the Court finds that there is reason to believe that notification of the existence of this warrant will result in the destruction of or tampering with evidence, danger to the physical safety of an individual, flight from prosecution, and/or intimidation of potential witnesses, or otherwise will seriously jeopardize an ongoing investigation. Accordingly, it is hereby ordered that the Provider shall not disclose the existence of this Warrant and Order to the listed subscriber or to any other person for a period of 180 days from the date of this Order, subject to extension upon application to the Court if necessary, except that Provider may disclose this Warrant and Order to an attorney for Provider for the purpose of receiving legal advice.


**3. Sealing.** It is further ordered that this Warrant and Order, and the Affidavit upon which it was issued, be filed under seal, except that the Government may without further order of this Court serve the Warrant and Order on the Provider; provide copies of the Affidavit or Warrant and Order as need be to personnel assisting the Government in the investigation and prosecution of this matter; and disclose these materials as necessary to comply with discovery and disclosure obligations in any prosecutions related to this matter.

**4. Expedited Compliance.** The Provider shall comply with this Order, and provide all information to the Investigating Agency as directed herein, within twenty-four hours of receipt of this Order *if feasible.*

Dated: New York, New York

*May 19, 2017*  
Date Issued

*2:56pm*  
Time Issued

  
HONORABLE GABRIEL W. GORENSTEIN  
United States Magistrate Judge  
Southern District of New York

## **Search Attachment A**

### **I. Target Accounts and Execution of Warrant**

This warrant is directed to Facebook, Inc. (the “Provider”), headquartered in Menlo Park, California, and applies to all content and other information within the Provider’s possession, custody, or control associated with the following “Target Accounts”:

- a. The Facebook account with identification number 100013341277222;
- b. The Facebook account with identification number 503619729;
- c. The Facebook account with identification number 100007817464240;
- d. The Facebook account with identification number 1602196647;
- e. The Facebook account with identification number 547052076;
- f. The Facebook account with identification number 1656786545;
- g. The Facebook account with identification number 54700693;
- h. The Facebook account with identification number 1417299773;
- i. The Facebook account with identification number 564327740; and
- j. The Facebook account with identification number 551231921.

A law enforcement officer shall serve this warrant by transmitting it via email or another appropriate manner to the Provider. The Provider is directed to produce to the law enforcement officer an electronic copy of the information specified in Section II below. Upon receipt of the production, law enforcement personnel will review the information for items falling within the categories specified in Section III below, a copy of which shall not be transmitted to the Provider.

### **II. Information to be Produced by the Provider**

To the extent within the Provider’s possession, custody, or control, the Provider is directed to produce the following information associated with each **Target Account**:

- a. All contact and personal identifying information, including full name, user identification number, birth date, gender, contact e-mail addresses, Facebook passwords, Facebook security questions and answers, physical address (including city, state, and zip code), telephone numbers, screen names, websites, and other personal identifiers.
- b. All activity logs for the account and all other documents showing the user's posts and other Facebook activities;
- c. All photos and videos---and all associated metadata---uploaded by the user of the Target Account and all photos and videos uploaded---and all associated metadata---by any user that have that user tagged in them;
- d. All profile information (including Neoprint); News Feed information; status updates; links to videos, photographs, articles, and other items; Notes; Wall postings; friend lists, including the friends' Facebook user identification numbers; groups and networks of which the user is a member, including the groups' Facebook group identification numbers; future and past event postings; rejected "Friend" requests; comments; gifts; pokes; tags; and information about the user's access and use of Facebook applications;
- e. All other records of communications and messages made or received by the user---and all associated metadata and embedded emoticons---including all private messages, chat history, video calling history, and pending "Friend" requests;
- f. All "check ins" and other location information;
- g. All IP logs, including all records of the IP addresses that logged into the Target Account;
- h. All records of the Target Account's usage of the "Like" feature, including all Facebook posts and all non-Facebook webpages and content that the user has "liked";

- i. All information about the Facebook pages that the Target Account is or was a “fan” of;
- j. All past and present lists of friends created by the Target Account;
- k. All records of Facebook searches performed by the Target Account;
- l. All information about access and use of Facebook Marketplace by the user of the Target Account;
- m. The types of service utilized by the user of the Target Account;
- n. The length of service (including start date) and the means and source of any payments associated with the service (including any credit card or bank account number);
- o. All privacy settings and other account settings, including privacy settings for individual Facebook posts and activities, and all records showing which Facebook users have been blocked by the account;
- p. All records pertaining to communications between Facebook and any person regarding the user or the user’s Facebook account, including contacts with support services and records of actions taken.
- q. Preserved records. Any preserved copies of any of the foregoing categories of records created in response to any preservation request(s) issued pursuant to 18 U.S.C. § 2703(f).

### **III. Review of Information by the Government**

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the records produced by the Provider in order to locate any evidence, fruits, and instrumentalities of violations of: (i) Title 18, United States Code, Section 2339B (providing material support or resources to designated foreign terrorist organizations); (ii) Title 18, United

States Code, Section 2339D (receipt of military-type training from designated foreign terrorist organizations); (iii) Title 18, United States Code, Section 924(c) (firearms offenses related to crimes of violence); (iv) Title 18, United States Code, Section 1001 (making false statements or omissions in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States); and (v) Title 18, United States Code, Section 1425 (procurement of citizenship or naturalization unlawfully) (the “Subject Offenses”), including the following:

- a. Communications relating to the Subject Offenses, including communications relating to the provision of support to Hizballah, the receipt of military-type training from Hizballah, taskings on behalf of Hizballah, surveillance conducted for Hizballah, the use and acquisition of weapons, and the making of false statements to the U.S. government;
- b. Evidence or communications related to purchases or efforts to acquire bomb components and/or chemical precursors for bombs;
- c. Evidence relating to the acquisition of U.S. travel documents or visas for travel to countries outside of the United States;
- d. Videos, posting, or communications pertaining in any way to Hizballah or other terrorist organizations;
- e. Evidence of Hizballah’s structure, membership, objectives, or other activities, including but not limited to evidence of Hizballah’s designation as a foreign terrorist organization, and the fact that Hizballah engages in or has engaged in terrorist activities;
- f. evidence of the identity(ies) of the user(s) of the Target Accounts;

- g. evidence of the identities and locations of co-conspirators in the Subject Offenses, including photographs of and communications with such individuals;
- h. evidence of participation in the Subject Offenses by the user(s) of the Target Accounts and others, including records and photographs relating to travel and financial transactions in furtherance of the Subject Offenses;
- i. evidence related to banks and other financial institutions at which the user(s) of the Target Accounts conducts business, including, potentially, transactions in furtherance of the Subject Offenses;
- j. evidence of other online accounts and email addresses used by the user(s) of the Target Accounts, including potentially for operational activity or otherwise in furtherance of the Subject Offenses; and
- k. passwords or other information needed to access user's computer or other online accounts.